Secure Intrusion Detection System of Denial of Service Attack Using Multivariate Correlation Analysis

Nischitha KC
4th sem Mtech, Dept of CSE, SJBIT
Bangalore, India

Mr. Dhananjaya M
Associate Professor, Dept of CSE, SJBIT
Bangalore, India

***Abstract*---Denial-of-Service (DoS) attack are one of the most common threat to the online servers such as web servers, cloud computing servers, database servers etc, which makes the machine or network resources unavailable to its intended users. Such type of attack can be detected using a system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting geometrical correlations between network traffic features. The MCA based detection system utilizes the principle of anomaly based detection in recognizing the attack. This will help in detecting the known and unknown DoS attack by learning the patterns of legitimate network traffic.**

I. INTRODUCTION

Denial of Service (DoS) attack are the kind of dangerous intrusive behavior that cause a serious damage to online servers such as cloud computing servers, web servers, database servers etc. DoS attack attempts to make the network resources such as host, router, or the entire network unavailable to its intended users. It imposes an intensive computational task to victim by exploiting the system vulnerability or flooding it with large amount of unwanted packets which would cause the victim to force out of the service. This reduces the efficiency of the online services and hence detection of such attacks is required to protect the online services.

Intrusion detection system can be classified into network based detection system and host based detection system. A network based detection system focus on protecting network information assets. Host based detection system focus on protecting server or hosts information assets. The DoS attack detection system mainly focus on development of network based detection mechanism. Such mechanism works on monitoring the protected network for traffic transmitted over them. They release the protected online servers from monitoring attacks and make sure that the servers would dedicate themselves to provide quality of service with less delay in response. The network based detection systems are loosely coupled with operating system running on the host system which they are protecting and hence configurations of network based detection system are less complicated than that of host based detection systems.

The network based detection system can be classified into two main categories namely misuse based detection system and anomaly based detection system. The misuse based detection system examines network traffic in search of patterns that match known signatures which are preconfigured, predetermined attack patterns. The problem with the misuse based detection approach is that as new attack strategies are identified the database of signature must be continually updated otherwise attacks that use new strategies will not be recognized and might succeed. Another weakness of the misuse based detection method is that a slow, methodical attack might escape detection if the relevant attack signature has a shorter time frame. Instead of having high detection rates to known attacks and low false positive rates, misuse detection systems have low detection rate n high false positive rates. The anomaly based detection system monitors the network activity and flags any network activity presenting significant deviation from legitimate traffic profiles as suspicious objects. It helps in detecting zero day intrusions which exploits previous unknown system vulnerabilities. The anomaly based detection system helps in detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic.

II. SYSTEM ARCHITECTURE

A. Framework

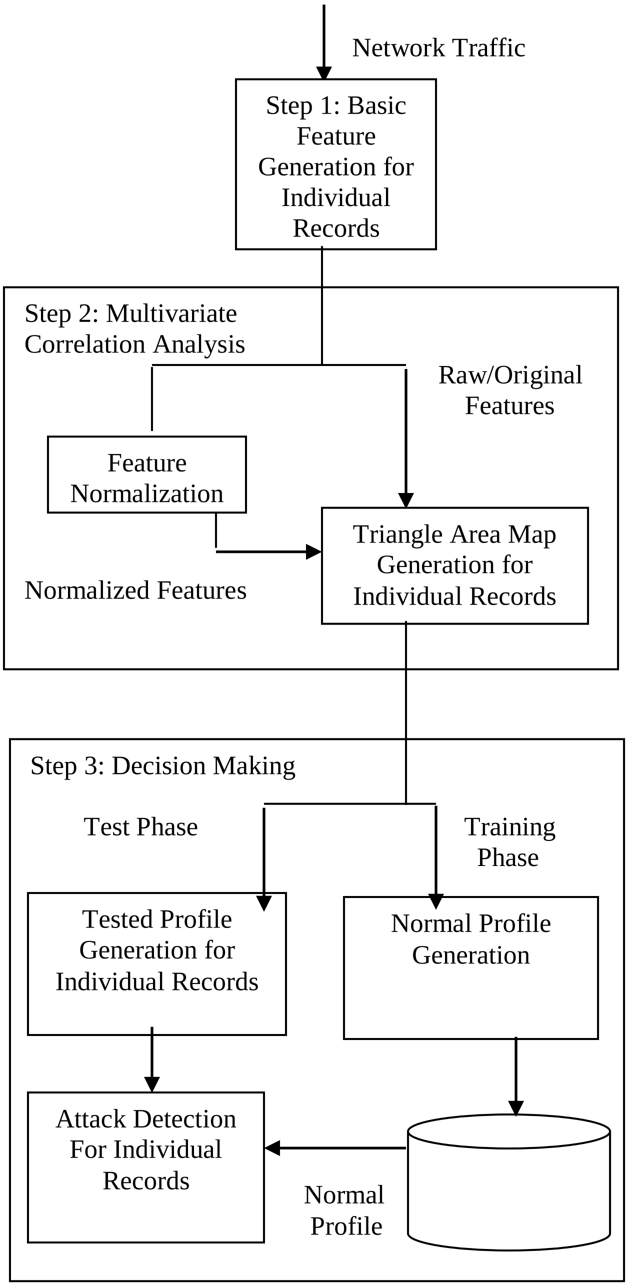
Network Traffic
Step 1: Basic Feature Generation for Individual Records
Step 2: Multivariate Correlation Analysis
Raw/Original Features
Feature Normalization
Triangle Area Map Generation for Individual Records
Normalized Features
Step 3: Decision Making
Test Phase
Training Phase
Tested Profile Generation for Individual Records
Normal Profile Generation
Attack Detection For Individual Records
Normal Profile

Fig 2.1 Framework of the proposed denial of service attack detection system

Fig 2.1 shows the overview of the proposed DoS attack detection system and it consists of three major steps. The sample by sample detection mechanism is involved in the entire detection phase.

In first step the basic features for individual records are generated from network traffic to the internal network in which protected servers reside and they are used to form traffic records. The destination network is analyzed and monitored in order to reduce overhead of detecting malicious activities by concentrating on relevant inbound traffic which also enable the detector to give protection that suits the targeted internal network since the legitimate traffic profiles used by the detectors are developed for smaller number of network services.

The second step is the multivariate correlation analysis. In this step the triangle area map generation module is operated to get correlations between two distinct features within each traffic record arriving from first step or traffic record normalized by the feature normalization module in second step. If any network intrusion has occurred then it cause changes to the correlations and those changes can be used as indicators to recognize the intrusive activities. The extracted correlations namely triangle areas stored in Triangle Area Maps (TAMs) are used to replace the original basic features or normalized features to represent the traffic records and this provides greater discriminative information that differentiate between legitimate and illegitimate traffic records.

The third step is the decision making in which anomaly based detection mechanism is adopted. It helps in detecting any of the DoS attack without having any attack relevant knowledge and avoids the labor intensive attack analysis and the frequent update of the attack signature database as in case of misuse based detection. The mechanism used in this step improves the robustness of the proposed detectors and it is difficult for the attackers to generate attacks that match the normal traffic profiles that are built by specific detection algorithm. There are two phases in this step namely training phase and test phase. The normal profile generation module is operated in training phase which generates profiles for various types of legitimate traffic records and stored in database. The tested profile generation module operated in test phase generates the profile for individual observed traffic records. These tested profiles are given to attack detection module that compares the individual tested profile with stored normal profile. A threshold classifier is used in attack detection module to distinguish DoS attack from legitimate traffic.

B. Sample by Sample Detection

When compared to the sample by sample detection mechanism the group based detection mechanism has higher probability in classifying the groups of sequential network traffic samples. But the proof of group based detection mechanism was based on assumption that the samples were taken from the same distribution or class which restricts the group based detection to limited scenarios since attack may occur unpredictably and might be difficult to obtain the group of sequential samples only from the same distribution. In order to remove such restriction the proposed system investigates traffic samples individually.

III. MULTIVARIATE CORRELATION Analysis

The behavior of the DoS attack from the legitimate network traffic is different and such behavior of network traffic is reflected by its statistical properties. In order to describe these statistical properties the Multivariate Correlation Analysis (MCA) approach is presented. The MCA approach uses triangle area to extract the correlative information between the features within the observed data object. A Triangle Area Map (TAM) is constructed and all of the triangle areas are arranged on the map with respect to their indexes. The values of the elements are set to zero on the diagonal of the map since only correlation between each pair of distinct features is required. The two of the TAM are compared and they can be viewed as two images having their diagonals symmetric and any difference found in the upper triangle can be found on their lower triangle of the images. Hence to compare of the two TAM either upper or lower triangle can be chosen. Therefore the MCA approach provides the following benefits for the purpose of data analysis. Firstly the knowledge of historic traffic in performing analysis is not required. Secondly the triangle area based MCA withstand the problem of vulnerability to linear change to all the features. Third it provides characterization for individual network traffic records rather than model network traffic behavior of a group of network traffic records which results in lower latency in decision making and enables sample by sample detection. Fourth the correlations between distinct pairs of features are showed through the geometrical structure analysis and changes to these structures occur when anomaly behavior appear in the network which provides an important signal to trigger an alert.

IV. DETECTION MECHANISM

A threshold based anomaly detector is presented where normal profiles are generated using purely legitimate network traffic records which are utilized for upcoming comparisons with that of the new incoming investigated traffic records. The dissimilarity between normal profile and new incoming traffic record is checked by the proposed detector and if the dissimilarity is greater than a predetermined threshold then the traffic record is flagged as attack else it is labeled as legitimate traffic record. The threshold and normal profiles have direct influence on the performance of threshold based detector. The normal profiles with low quality results in inaccurate characterization to legitimate network traffic hence triangle area based MCA approach is applied in order to analyze legitimate network traffic and the generated TAM are used to supply quality features for normal profile generation.

V. RESULT

The system will end up with blocking the user who is trying to attack (DoS or SQL injection) on the system. The blocking will be of two types, permanent blocking and temporary blocking. The threshold value has been decided depending on impact of the attack. If the current attack value is more than threshold then user will be blocked permanently and if it is less than threshold then he will be notified about his behavior on the network and will be able to request the admin to unblock his services. Admin has the privilege to remove temporary blocking.

VI. CONCLUSION

This paper has presented a MCA-based DoS attack detection system which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The former technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviours. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

To be part of the future work, we will further test our DoS attack detection system using real world data and employ more sophisticated classification techniques to further alleviate the false positive rate.

VI. REFERENCES

[1] V. Paxson, “Bro: A System for Detecting Network Intruders in Realtime,” *Computer Networks*, vol. 31, pp. 2435-2463, 1999

[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, “Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges,” *Computers & Security*, vol. 28, pp. 18-28, 2009.

[3] D. E. Denning, “An Intrusion-detection Model,” *IEEE Transactions on Software Engineering*, pp. 222-232, 1987.

[4] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attack detection method using cluster analysis,” Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, “Intrusion detection using fuzzy association rules,” Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[6] J. Yu, H. Lee, M.-S. Kim, and D. Park, “Traffic flooding attack detection with SNMP MIB using SVM,” Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[7] W. Hu, W. Hu, and S. Maybank, “AdaBoost-Based Algorithm for Network Intrusion Detection,” Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.

[8] C. Yu, H. Kai, and K. Wei-Shinn, “Collaborative Detection of DDoS Attacks over Multiple Network Domains,” Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.

[9] G. Thatte, U. Mitra, and J. Heidemann, “Parametric Methods for Anomaly Detection in Aggregate Traffic,” Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

[10] S. T. Sarasamma, Q. A. Zhu, and J. Huff, “Hierarchical Kohonenen Net for Anomaly Detection in Network Security,” *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 35, pp. 302-312, 2005.

[11] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, “Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient,” Parallel and Distributed Systems, IEEE Transactions on, vol. 23, pp. 1073-1080, 2012.

[12] S. Jin, D. S. Yeung, and X. Wang, “Network Intrusion Detection in Covariance Feature Space,” *Pattern Recognition*, vol. 40, pp. 2185-2197, 2007.

[13] C. F. Tsai and C. Y. Lin, “A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection,” *Pattern Recognition*, vol. 43, pp. 222-229, 2010.

[14] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, “RePIDS: A multi tier Real-time Payload-based Intrusion Detection System,” Computer Networks, vol. 57, pp. 811-824, 2013.

[15] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “Denialof- Service Attack Detection Based on Multivariate Correlation Analysis,” Neural Information Processing, 2011, pp. 756-765.

[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “Triangle- Area-Based Multivariate Correlation Analysis for Effective Denial of-Service Attack Detection,” The 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012, pp. 33-40.

[17] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, “Costbased modeling for fraud and intrusion detection: results from the JAM project,” The DARPA Information Survivability Conference and Exposition 2000 (DISCEX ’00), Vol.2, pp. 130-144, 2000.

[18] G. V. Moustakides, “Quickest detection of abrupt changes for a class of random processes,” Information Theory, IEEE Transactions on, vol. 44, pp. 1965-1968, 1998.

[19] A. A. Cardenas, J. S. Baras, and V. Ramezani, “Distributed change detection for worms, DDoS and other network attacks,” The American Control Conference, Vol.2, pp. 1008-1013, 2004.

[20] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, “Attribute Normalization in Network Intrusion Detection,” The 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009, pp. 448-453.